


Tuya may be the China threat that beats Russia's ransomware attacks

 thehill.com/opinion/cybersecurity/564962-tuya-may-be-the-china-threat-that-beats-russias-ransomware-attacks

July 30, 2021

Opinion>Cybersecurity

The views expressed by contributors are their own and not the view of The Hill

 Cyber war has a new weapon: Your smartphone

Getty Images

In May, Americans lined up at gas stations for days because of a Russian ransomware attack. Recently, a similar Russia-sourced attack struck a large group of companies via software used by IT departments to manage remote computers. But those attacks are about money, not about power or information, and a little-known Chinese technology company, Tuya, is on the verge of being able to blow Russian hackers away.

Tuya, a nominally private Chinese company backed by Beijing-government crony Tencent, takes “things” and makes them “smart” by connecting them to the internet, a function known as “platform as a service,” or PaaS. Tuya dominates the global “internet of things” (IoT)/PaaS market. It operates from Hangzhou City, China, and its hardware, software, cloud services and applications power more than 100 million “smart” devices in 1,100 product categories in 220 countries — including consumer products, surveillance equipment, and manufacturing and supply chain applications.

More than 600 of the world’s leading brands use the company to power their own IoT devices sold at Walmart, Nordstrom, Amazon, Target and elsewhere. Tuya’s market domination translated into a March 2021 listing on the New York Stock Exchange and more than \$900 million in new investment. Strangely, however, that access has brought little scrutiny — even in light of new focus on Chinese efforts to corner the market in next-gen tech.

Over the past few years, the United States and at least 20 other countries have either banned or significantly restricted China’s Huawei telecommunications company from building or managing 5th Generation (5G) networks. Their motive? Fear that the company could siphon the masses of data — including classified government data — created and shared on its networks, and make it available to the Chinese government.

Remember, China’s Data Security Law dictates that both private and state or partially state-owned or controlled corporations must cede control over user data to the Beijing government.

The alarm that has spread from Washington to Europe and Asia over 5G makes sense. The technology means an unprecedented 20-fold increase in data flow. And it is just that expansion that is enabling the rapidly exploding internet of things, and a world where the internet is omnipresent. Enter Tuya. This one Chinese company alone soon may control hundreds of millions more “smart” devices enabled by 5G — even non-Huawei 5G — essentially rolling back any progress made in defending proprietary personal or government data from China’s ruling Communist Party.

A recent investigation by cybersecurity firm Dark Cubed found that Tuya-powered devices “had at least one network connection to servers based in China ... failed basic security checks ... provided complete visibility into private images to anyone in the network ... [and] are

woefully insecure and sending data to China.” In other words, Tuya may well be funneling the information picked up on home security cameras and connected health devices — just to name two examples — back to Beijing.

U.S. law makes it illegal for companies to provide this data to the Chinese government, but enforcing that law is difficult — especially when Beijing assists companies in hiding their actions. Meanwhile, naysayers insist all such arguments are little more than alarmism or xenophobia. But consider the precedents.

In 2009, the Dutch telecommunications company KPN used technology provided by Huawei in its networks. An internal risk assessment, which only came to light years later, reportedly concluded that this access allowed Huawei to monitor all conversations on KPN networks, including those by the Dutch prime minister. And the internet of things only adds vulnerability: In 2016, the so-called Mirai botnet attack took over more than 600,000 smart devices and used them to temporarily shut down much of the internet on the East Coast. That attack was the work of criminals, but it foreshadows the sort of trouble a determined state actor — with access to a far larger number of devices — could cause.

Fortunately, the United States has options. The Biden administration has extended a 2019 Executive Order on Securing the Information and Communications Technology and Services (ICTS) Supply Chain, which gives the Secretary of Commerce the authority to review — and deny — “any acquisition, importation, transfer, installation, dealing in, or use of any [ICTS products] that has been designed, developed, manufactured, or supplied” by persons owned, controlled, subject to, or at the direction of foreign adversaries, which “poses certain undue or unacceptable risks.”

Tuya appears to meet that definition and Congress should consider barring it from operating in the United States and from doing business with U.S. companies. There are alternative IoT/PaaS offerings from companies in the U.S. and other trusted nations. It’s time for better U.S. leadership, before it’s too late.

Hal Brands is a senior fellow at the American Enterprise Institute, where he studies U.S. foreign policy and defense strategy, and a professor at the Johns Hopkins University School of Advanced International Studies.

Klon Kitchen is a senior fellow at the American Enterprise Institute, where he studies emerging technologies and national security. He is an adviser to Afero, an American IoT/PaaS company.

Editor’s note: In response to this article, Tuya states that, since March 2021, it has been a publicly traded Chinese company whose investors include Tencent, operating internationally with local headquarters in the U.S., India, Germany, Colombia, China and Japan. Regarding the potential for sharing data with the Beijing government, Tuya states that all user data on its platform is assigned to specific regional data centers, according to

the users' locations, and that servers operate independently with no connection to China. Regarding IoT devices and 5G technology, Tuya states that the consumer IoT devices it supports do not use 5G technology related to base station infrastructure and have no cooperation or association with Huawei or other 5G technology service providers. And regarding the investigation by Dark Cubed, Tuya says the IPC products mentioned in the report are not devices developed by Tuya and the specific domain requested by those products belongs to the IPC manufacturer. Tuya says it welcomes fair-market competitions around the globe, to facilitate healthy and orderly IoT development.